CLAIMS

We claim:

1. A apparatus for key management comprising:

(a) a multitude of key registers;

(b) a multitude of type fields, wherein each type field is associated with a key registers;

(c) a key management controller;

(d) key management algorithms; and

(e) key management functions.

2. The apparatus according to claim 1 wherein each type field contains at least one of the values including KK, DK, and null.

3. The apparatus according to claim 2 wherein the contents of a key register with an associated type field whose value is KK is used to encrypt and decrypt the contents of other key registers.

4. The apparatus according to claim 1 wherein said key management functions include an unwrap function, said unwrap function including:

(a) a wrapped key parameter for specifying an unwrapping key;

(b) a type parameter for specifying an unwrapping key type;

(c) an index parameter for specifying where to store the unwrapped key; and

(d) a wrapped key index parameter for specifying a wrapped key;

said unwrap function capable of unwrapping the wrapped key using the specified unwrapping key and an algorithm determined by the unwrapping key type.

5. The apparatus according to claim 1 wherein said key management functions include a wrap function, wherein said wrap function includes:

(a) an index parameter for specifying a wrapping key; and

(b) a wrapping key index parameter for specifying a wrapping key key;

said wrap function capable of wrapping the wrapping key using the specified wrapping key key.

6. The apparatus according to claim 1 wherein said key management functions include a data encryption function, said data encryption function includes:

(a) a data parameter for specifying encryption data; and

(b) a key index parameter for specifying an encryption key;

said encryption function capable of encrypting the specified encryption data using the specified encryption key.

7. The apparatus according to claim 1 wherein said key management functions include a data decryption function, wherein said data decryption function includes:

(a) a cipher parameter for specifying a cipher for decryption; and

(b) a key index parameter for specifying a decryption key;

said decryption function capable of decrypting the specified cipher using the specified decryption key.

8. The apparatus according to claim 1 wherein said key management functions include a data load function, wherein said data load function includes:

(a) a key parameter for specifying a plaintext key; and

(b) an index parameter for specifying a destination key register;

said data load function capable of loading the specified plaintext key into the destination key register.

9. The apparatus according to claim 1 wherein said key management functions include a register clear function, wherein said register clear function includes an index parameter for specifying a key register, and is capable of clearing the specified key register and an associated type field.

10. The apparatus according to claim 1 wherein said key management functions include an initialize function, wherein said initialize function is capable of:

(a) clearing said multitude of key registers;

(b) storing a specified plaintext key in an indexed register; and

(c) storing a KK value in the type field associated with the indexed register.

11. The apparatus according to claim 1 wherein said multitude of key registers has a hierarchy.

12. The apparatus according to claim 11 wherein said contents of a key register can only be used to wrap the contents of a lower hierarchical level key register.

13. The apparatus according to claim 11 wherein said hierarchy has more than one root.

14. The apparatus according to claim 1 wherein a key management function uses a key management algorithm determined by the value stored in the type field associated with the key register being operated on by said key management function.

15. The apparatus according to claim 1 wherein said apparatus uses public key negotiation protocols to share new keys with other key management apparatuses.

16. The apparatus according to claim 1 wherein said key management algorithms includes an encryption algorithm for wrapping a DK with a KK, wherein the wrapped data key = $E_{KK}(E_{KK}(DK))$.

17. The apparatus according to claim 1 wherein said key management algorithms include a decryption algorithm for unwrapping a DK with a KK, wherein the wrapped data key = $E_{KK}(E_{KK}(DK))$.

18. The apparatus according to claim 1 wherein said key management algorithms include encryption and decryption algorithms that use a bitwise exclusive-or operator.

19. A method for key management comprising the steps of:

(a) storing a data key in a key register;

(b) storing an data type for said data key in an associated type field;

(c) storing a key key in a key register;

(d) storing a key type for said key key in an associated type field; and

(e) performing a key management function on at least one key register using a key management algorithm.

20. The method according to claim 19 wherein said data type is at least one of the values including KK, DK, and null.

21. The method according to claim 19, wherein said step of performing a key management function includes performing an unwrap function, said unwrap function includes the steps of:

(a) retrieving an unwrapping key from a key register;

(b) retrieving an unwrapping key type;

(c) determining where to store an unwrapped key;

(d) retrieving a wrapped key; and

(e) unwrapping the wrapped key using the unwrapping key and an algorithm determined by the unwrapping key type.

22. The method according to claim 19, wherein said step of performing a key management function includes performing a wrap function, wherein said wrap function includes the steps of:

(a) retrieving a wrapping key;

(b) retrieving a wrapping key key; and

(c) wrapping the wrapping key using the wrapping key key.

23. The method according to claim 19, wherein said step of performing a key management function includes performing a data encryption function, said data encryption function includes the steps of:

(a) retrieving data for encryption;

(b) retrieving an encryption key; and

(c) encrypting the data using the encryption key.

24. The method according to claim 19, wherein said step of performing a key management function includes performing a data decryption function, wherein said data decryption function includes the steps of:

(a) retrieving a cipher;

(b) retrieving a decryption key; and

(c) decrypting the cipher using the decryption key.

25. The method according to claim 19, wherein said step of performing a key management function includes performing a data load function, wherein said data load function includes the steps of:

(a) retrieving a plaintext key;

(b) determining a destination key register; and

(c) loading the specified plaintext key into the destination key register.

26. The method according to claim 19, wherein said step of performing a key management function includes performing a register clear function, wherein said register clear function includes the steps of:

(a) clearing a specified key register; and

(b) clearing an associated type field.

27. The method according to claim 19, wherein said step of performing a key management function includes performing an initialize function, wherein said initialize function includes the steps of:

(a) clearing a multitude of key registers;

(b) storing a specified plaintext key in an indexed key register; and

(c) storing a KK value in the type field associated with the indexed register.

28. The method according to claim 19, wherein said key register is part of a hierarchy of key registers.

29. The method according to claim 28, wherein said contents of the key register can only be used to wrap the contents of a lower hierarchical level key register.

30. The method according to claim 28, wherein said hierarchy has more than one root.

31. The method according to claim 19, wherein the step of performing a key management function further includes using a key management algorithm determined by the value stored in the type field associated with the key register being operated on by said key management function.

32. The method according to claim 19, further including the step of sharing new keys with other key management apparatuses using public key negotiation protocols.